RL-TR-97-41
Final Technical Report
July 1997

SYNTHESIS OF POWER PLANT OUTAGE SCHEDULES

Kestrel Institute

Douglas R. Smith

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

Rome Laboratory
Air Force Materiel Command
Rome, New York

This report has been reviewed by the Rome Laboratory Public Affairs Office (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

RL-TR-97-41 has been reviewed and is approved for publication.

APPROVED:

LOUIS J. HOEBEL
Project Engineer

FOR THE COMMANDER:

JOHN A. GRANIERO, Chief Scientist
Command, Control & Communications Directorate

If your address has changed or if you wish to be removed from the Rome Laboratory mailing list, or if the addressee is no longer employed by your organization, please notify RL/C3CA, 525 Brooks Rd, Rome, NY 13441-4505. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document require that it be returned.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	JULY 1997	Final Apr 95 - Jan 96

4. TITLE AND SUBTITLE

SYNTHESIS OF POWER PLANT OUTAGE SCHEDULES

5. FUNDING NUMBERS

C - F30602-95-C-0063
PE - 62702F
PR - 5581
TA - 27
WU- PU

6. AUTHOR(S)

Douglas R. Smith

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Kestrel Institute
3260 Hillview Ave.
Palo Alto, CA

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Rome Laboratory/C3CA
525 Brooks Rd.
Rome, NY 13441-4505

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

RL-TR-97-41

11. SUPPLEMENTARY NOTES

Rome Laboratory Project Engineer: Louis J. Hoebel/C3CA/315-330-3655

12a. DISTRIBUTION AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This document provides a report on the creation of domain theories in the power plant outage domain. These were developed in conjunction with the creation of a demonstration system of advanced scheduling technology for the outage problem.

14. SUBJECT TERMS

Scheduling, Domain Theories

15. NUMBER OF PAGES

20

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Standard Form 298 (Rev. 2-89) (EG)
Prescribed by ANSI Std. 239.18
Designed using Perform Pro, WHS/DIOR, Oct 94

1 Overview

In 1994 personnel from Rome Laboratory (RL), Kaman Science (KS), Kestrel Institute, and the Electric Power Research Institute (EPRI) began a joint project to develop scheduling tools for power plant outage activities. This report describes our support for this joint effort. The project uses KIDS (Kestrel Interactive Development System) to generate schedulers from formal specifications of the power plant domain outage activities.

2 Technical Approach

The Kestrel Interactive Development System (KIDS) provides automated support for the development of correct and efficient programs from formal specifications. The system has components for performing algorithm design, deductive inference, program simplification, partial evaluation, finite differencing optimizations, data type refinement, compilation, and other development operations. KIDS has been used to design and optimize many programs, including a variety of high-performance schedulers in the transportation domain.

Building a domain theory for power plant maintenance activities is the most time-consuming part of producing useful scheduling tools. It requires defining sorts, operations, and axioms that capture the basic concepts of the domain and the laws for reasoning about them. The domain theory then provides the vocabulary for writing specifications for particular scheduling problems. Once the theory and problem specifications have been developed (and this is usually an iterative process), KIDS can be used to generate executable code from the specifiation. We have built over a hundred theories for various application domains and common mathematical and data structures. We have used KIDS to synthesize many programs, many of which are comparable or better than manually produced programs.

Kestrel personnel assisted in the following aspects of the project. Details may be found in the attached technical report.

- *Building a domain theory* – This involved defining the basic concepts of the domain, writing a formal specification of the outage scheduling problem, providing laws for specific terms in the specification, and developing a global search theory for outage scheduling. The result is about 2000 lines of Refine text.
- *Deriving propagation constraints for safety constraint* – The safety constraints are key to the success of an outage scheduler. It turns out that their form is unusual and required a generalization of our previously developed methodology for inferring propagation constraints. Drs. Gomes and Smith worked out various versions of these constraints during the project. Many hours were spent carefully working out mathematical calculations on paper, which were then summarized as lemmas in the domain theory.

- *Extending the constraint propagation code generator* – The new class of propagation constraints arising from the safety constraint required extensions to the constraint propagation code generator which were performed by Dr. Westfold.

- *Developing an interface for the ATOSS system* – Finally, in order to have a usable system, we adapted the CLIM interface that Kestrel developed for KTS (Kestrel Transportation Scheduler) to the needs of outage scheduling, resulting in the ATOSS system that was demonstrated at the Utility workshop in December 1995.

Under separate contracts we continue to develop the theory and implementation techniques that apply to the kind of resources and constraints that arise in power plant outage scheduling. We hope to continue our support for the development of ATOSS.

Challenges in Deploying Planning and Scheduling Systems: Outage Management of Nuclear Power Plants

Carla P. Gomes
Rome Laboratory*
525 Brooks Rd.
Rome Lab, NY 13441-4505
gomes@ai.rl.af.mil

Douglas Smith and Stephen Westfold
Kestrel Institute
3260 Hillview Avenue
Palo Alto, CA 94304
{smith,westfold}@kestrel.edu

Abstract

We address the challenges of deploying AI planning and scheduling systems in real world environments. In particular, we discuss the management of refueling outages of nuclear power plants, a domain for which the existence of good automatic solutions is not only crucial for nuclear safety reasons but also for economic reasons — the cost of each day of shutdown is in the order of $1,000,000. We report on a successful project for transference of advanced planning and scheduling technology for outage management, a collaboration between Rome Laboratory, the Electrical Power Research Institute (EPRI), Kaman Science, and Kestrel Institute as part of DOD's dual-use program.

Statement:
Our current system handles up to 2,000 activities and was completed in November 1995. In December, we gave a demonstration of the system to the the management of several large utilities (American Electric Power, Pennsylvania Power & Light, GPU Nuclear Co., PECO, and others). The demonstration was successful, and EPRI will use the system to build the next generation of outage scheduling tools (referred to as the Advanced Technology Outage Scheduler).

Since our paper describes a successful prototype rather than a fully deployed system, we would like our work to be considered for inclusion on one of the panels or special sessions about *emerging* applications areas. (As per communication with Howard Shrobe, we understand that such panels are part of the plan to broaden the scope of *IAAI*.) We feel that the complexities and economic relevance of our application domain offer a unique application area for modern AI planning and scheduling techniques. Feel free to contact us (gomes@ai.rl.mil), if you have any further questions. Thank you for your consideration.

*Carla P. Gomes works for Rome Laboratory as a Research Associate.

1 Introduction

Planning and scheduling tasks are inherently complex. In computational terms, they are *intractable*, *i.e.*, NP-hard or worse. As a practical consequence, realistic size planning and scheduling problems cannot be solved optimally in a "reasonable" amount of time. Nonetheless, solutions have to be found for real-world problems, and therefore heuristic approaches have to be adopted, ideally with some guarantee on the quality of the solution.

We focus on the real-world problem of multiple resource-constrained project management. This problem is very common in manufacturing and it is a generalization of the well-known job-shop scheduling problem [Blazewicz *et al.* 83, Vaessens *et al.* 94]. As a particular instance of this problem, we consider the management of outages of nuclear power plants. An outage is a planned shutdown for refueling, repair, and maintenance. It is a rather daunting real-world task that may involve from 10,000 up to 45,000 activities. Furthermore, in this domain, the existence of good automatic solutions is not only crucial for nuclear safety reasons but also for economic reasons — the cost per day of shutdown is in the order of $1,000,000.

We report on a successful project for transference of advanced planning and scheduling technology for outage management, a collaboration between Rome Laboratory, the Electrical Power Research Institute, Kaman Science, and Kestrel Institute as part of DOD's dual-use program. The software environment selected for this project was KIDS (Kestrel Interactive Development System)[Smith 91], which is a set of semiautomatic tools to transform declarative problem specifications into correct and efficient programs. KIDS has been used to derive a fast transportation scheduler for the US Transportation Command, KTS (Kestrel Transportation Scheduler) [Smith & Parra 93]. KTS schedules 15,460 individual movement requirements in 71 cpu seconds on a Sparc 2. Furthermore, the resulting schedules produced by KTS have proven to be of good quality.

The main goal of the project was to evaluate the use of advanced AI planning and scheduling technology for management of outages of nuclear power plants. In this domain, risk and safety management are sine qua non conditions and therefore a planning and scheduling system (automatic or manual) has to enforce safety constraints guaranteeing that the state of the plant is safe at any time during an outage. The current automatic technology for outage scheduling used by the utilities does not incorporate safety requirements — currently, safety and risk management still heavily rely on manual rather than on automatic procedures. We adopt an integrated approach, by automatically enforcing safety constraints during the planning and scheduling phase. Our work shows that AI planning and scheduling techniques provide enough flexibility for capturing such a diverse and complex set of constraints in a large, real-world application.

The outage problem is modeled as a *constraint satisfaction problem* combining a *global*

search tactic with *constraint propagation.* We use a rich representation for the state of the plant at any time (as in planning approaches), which allows for efficient constraint-based reasoning, in particular, temporal reasoning (as in scheduling). The derivation of very specialized representations for the constraints to perform efficient propagation is a key aspect for the generation of very fast schedules — constraints are *compiled* into the code. In order to increase schedule robustness, our approach entails the generation of schedules that are feasible over time intervals rather than single time point start times.

In the next section, we describe the current state-of-the-art of outage management for nuclear power plants, and discuss its limitations. In section 3, we describe ROMAN, the prototype system developed by Rome Laboratory for Outage Management. Section 4 summarizes the main results achieved with ROMAN.

2 Outage Management of Nuclear Power Plants

Outage management of nuclear power plants has a great impact in terms of the outage costs (replacement power, labor cost, etc.) and implementation of safety procedures. Prior to 1979, before the accident at Three Mile Island, refueling was the driving factor behind outages of nuclear power plants: maintenance plans were governed by the projected duration of refueling activities. After the accident, the duration of outages became determined not only by refueling activities, but also by the work and plant modifications required to make the plant safer and more reliable [PSDI 94, Wallace 90]. Therefore, nowadays, refueling activities often no longer dictate the critical path in an outage.

Outage management of nuclear power plants can be stated as follows:

> Given a set of outage activities (refueling operations, repairs, modifications, and maintenance activities), a set of resources, and a set of technological constraints, assign times and resources to the activities in such way that the completion of the outage is minimized while safely performing all the activities required by the outage.

Depending on the planning and scheduling procedures of each particular plant, as well as the scope of the activities performed during the outage, the planning and scheduling of outages for nuclear power plants might involve from 10,000 up to 45,000 activities.

The general principle underlying the outage procedures is that outages should be as short as possible, maintaining the appropriate level of nuclear safety. In other words, the outage should be planned and managed to reduce shutdown risks through the appropriate consideration of preventive measures. The main safety functions and systems components that are monitored during an outage are: AC power control system,

primary and secondary containment, fuel pool cooling system, inventory control, reactivity control, shutdown cooling, and vital support systems.

2.1 Outage Management in the Real World

There are approximately 110 nuclear plants operating in the US, most of them are members of EPRI, the Electrical Power Research Institute. Outage management still heavily relies on the experience of the manual schedulers, rather than on automatic procedures. Current automatic approaches to outage management mainly consist of the application of project management techniques, such as PERT/CPM techniques.[1] Safety and risk assessment is usually a manual process which calls on the expertise of the personnel involved to make decisions based on published policies and procedures. In order to ensure that the sequence of activities performed during an outage follows the safety requirements, EPRI performs the risk assessment of the schedules generated by the utilities using a simulator that validates the schedule regarding safety functions by keeping track of the configuration of the plant at any time. If the schedules are not approved by EPRI, manual adjustments have to be performed in order to meet the safety requirements.

Even though the usage of project management techniques such as PERT/CPM constitutes a major improvement in the way outage management is performed in comparison to previous techniques, they suffer from major limitations due to the lack of consideration of safety constraints and the lack of speed to perform "what-if" scenarios.

3 ROMAN

Rome Laboratory in collaboration with the Electrical Power Research Institute, Kaman Science and Kestrel Institute developed a prototype for planning and scheduling of outages of nuclear power plants, ROMAN (Rome Laboratory Outage MANager), within the DOD's dual-use program [Gomes 96].

As we discussed in the introduction, ROMAN models the outage management problem as a constraint satisfaction problem combining a global search tactic with constraint propagation. The domain model of ROMAN includes all the technological constraints currently incorporated in the automatic tools used by the utilities for schedule generation. In addition, it includes all the constraints regarding the safety function AC power. Other safety functions could be modeled in a similar way. A top level formal specification of the outage problem as follows:

[1]The software currently used by the utilities to perform their outage planning and scheduling tasks are mainly: Primavera Project Planner for Windows (personal computers), Project/2 (mainframes), Project2/X for Windows (personal computers), Prestige (mainframes) and OpenPlan (personal computers).

function : *safe-outage-windows*(*activities*)
returns(*schedule* |
Consistent-Activity-Separation(*schedule*)*and*
Consistent-AC-power(*schedule*)*and*
All-activities-scheduled(*activities*, *schedule*))

In this formulation *activities* correspond to the set of activities to be performed. Each activity has a given duration, a set of predecessors (pred), and a set of effects on resources. The *schedule* is a partial order of activities. Activities in the schedule have time windows assigned to it. A time window defines the earliest start time (*est*) and latest start time (*lst*) of an activity, such that the activity can start at any time during the window without increasing the overall duration of the project. Given the duration of the activity, the earliest finish time (*eft*) and latest finish time (*lft*) can be calculated. The predicate *Consistent-Activity-Separation*(*schedule*) states that all the activities in the schedule satisfy the precedence constraints. The predicate *Consistent-AC-power*(*schedule*) states that the schedule verifies the safety constraints, from an AC power point of view. As a completeness condition, the predicate *All-activities-scheduled*(*activities*, *schedule*) states that all the activities have to be scheduled.

The notion of *state of the plant* is a key concept in enforcing safety constraints. In outage management the state of the plant is measured in colors — green, yellow, orange or red, in this order of increasing risk — and is computed by considering complex decision trees regarding safety levels as illustrated in Figure 1 for the safety function AC power control. For instance, if there is an activity being executed that has the potential to cause AC power loss, then in order for the plant to be in a yellow state it is required to have two off-site AC power sources available and three operable emergency safeguard buses.

Since the start times of activities are defined over time windows, we introduce two concepts regarding the execution of an activity: the *definite period* and the *potential period* of an activity. The definite period of an activity corresponds to the period of time during which the activity is definitely being execute — it is the time period between the latest start time of the activity (*lst*) and its earliest finish time (*eft*). The potential period of an activity corresponds to the period of time during which the activity may be executed — it is the time period between the earliest start time of the activity (*est*) and its latest finish time (*lft*). Figure 2 illustrates the notion of *definite* period of an activity. Notice that activity A does not have a definite period, since its earliest finish time is before its latest start time.

In addition, we define two other concepts: *definite state of the plant* and *potential state of the plant.* The definite state of the plant is associated with the concept of definite period: it represents the state of the plant for a given safety function (*e.g.*, AC power) assuming that activities are only executed during their definite period.

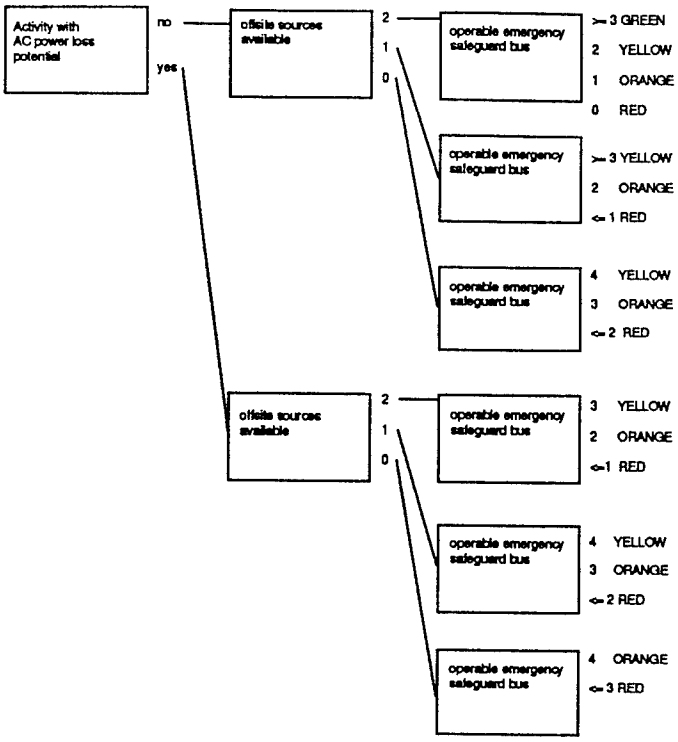

Figure 1: Example of a decision tree for the safety function AC Power

The concept of potential state of the plant is associated with the concept of potential period of an activity: it represents the state of the plant for a given safety function assuming that activities are executed during the whole extension of their potential period. The potential state of the plant is always "equal" or "greater" than the state of the plant since the definite period of an activity tends to underestimate the duration of activities while the potential period of an activity tends to overestimate the duration of activities. Figure 3 gives an example. Note that during certain time intervals, the definite and potential states of the plant coincide.

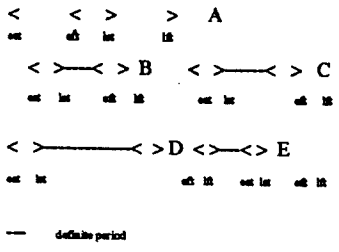

Figure 2: Notion of a definite period.

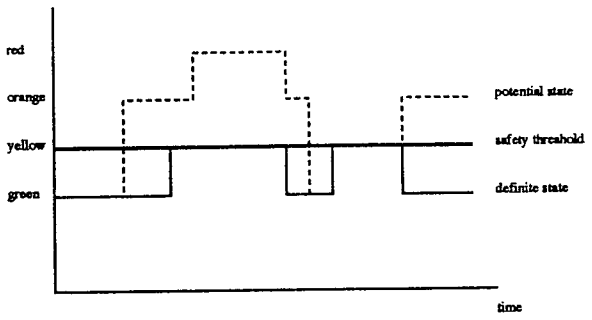

Figure 3: Definite and potential states of the plant.

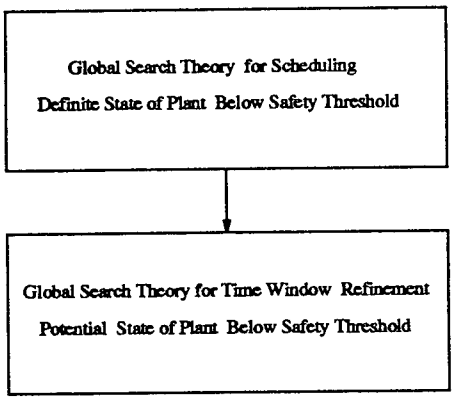

Figure 4: ROMAN's approach

3.1 Search and Control Mechanisms

KIDS provides algorithmic transformations that add control and search mechanisms to a given specification. The search tactic selected for the outage problem was *global search* [Smith 87, Smith *et al.* 95] (see also next section). Figure 4 summarizes the approach adopted in ROMAN.

Initially global search is applied to the formal specification of the outage problem in order to generate a schedule, assuming the definite period of activities. Since the notion of definite period tends to underestimate the duration of the activities, it is very likely for the schedule produced in this initial phase not to be feasible from the point of view of the potential state of the plant. In order to enforce the safety threshold for the potential state of the plant at any time during the outage, "refinement" of the time windows of the initial schedule takes place. In the next section, we describe our global search strategy.

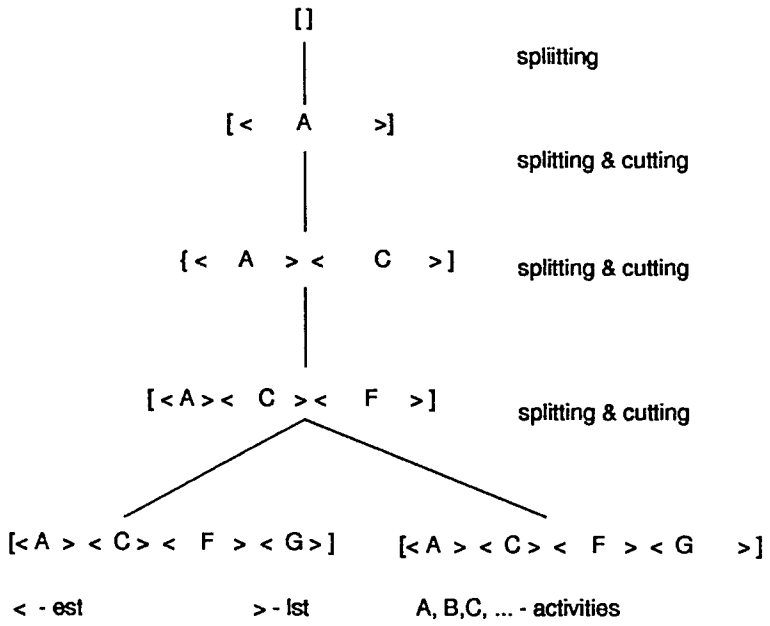

Figure 5: Global search theory for the Outage Problem (definite periods only).

3.1.1 Global Search Strategy

The *global search* tactic designs a backtrack strategy, based on an extension of "generate-and-test." The tactic is implemented by finding a space containing all the solutions to the problem that can be divided into nested subspaces. The global search algorithm starts with an initial set that contains all the solutions to the given problem instance, repeatedly extracts solutions, splits sets, and eliminates subsets using propagation, until no sets remain to be split. The process can be described as a tree search in which a node represents a set of candidates, and an arc represents the split relationship between a set and a subset. The principal operations are to extract candidate solutions from a set, and to split a set into subsets. The derivation of efficient cutting constraints that eliminate subspaces that do not contain any feasible solution is an important complementary operation in the derivation of the global search tactic.

Figure 5 illustrates the global search theory for the outage problem. In the case of global search theory for the initial scheduling of activities considering their definite periods the initial subspace descriptor (partial schedule) is the empty sequence (empty schedule). *Splitting* corresponds to appending an unscheduled activity, with a given time window, to the partial schedule. *Cutting* corresponds to propagating the constraints over the time windows of the activities in the partial schedule. Notice that cutting makes the time windows shrink. It can also split a time window as in the case of adding activity G — due to propagation, activity G's window was split into two. A candidate solution is *extracted* when all the activities have been scheduled.

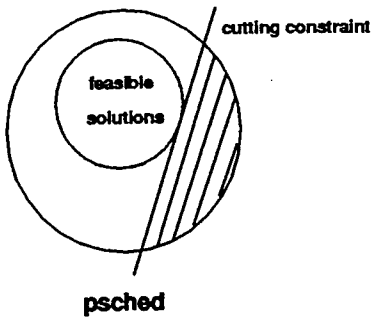

Figure 6: Cutting Constraints

As we can see from Figure 5, most of the work in this global search theory is performed by constraint propagation. Splitting corresponds to selecting the next activity to schedule. Figure 6 illustrates the concept of *cutting constraints* — *psched* is a partial schedule corresponding to a set of candidate solutions (*i.e.*, complete schedules). Cutting constraints remove portions of the search space that do not contain any feasible solution.

KIDS automatically instantiates a program scheme for global search with constraint propagation, incorporating cutting constraints. In order to take advantage of the propagation mechanisms provided in KIDS, the challenge lies in deriving the definition of the cutting constraints, normally a manual task. For more information on propagation in KIDS, see [Smith *et al.* 95]. For more information on cutting constraints for the outage problem, see [Gomes 96].

Refinement of time windows takes place if after applying the initial global search to the outage problem the potential state of plant does not satisfy the safety requirements. In other words, refinement of time windows is required to enforce the safety constraints over the potential period of all the activities in the initial schedule. This is achieved by applying a new global search to the formal specification of the outage with as input the schedule generated in the initial phase. In this second phase the windows of the activities that contribute to the contention periods, *i.e.*, the periods in which the potential state of the plant is above the safety threshold, are systematically reduced,[2] until the potential state of the plant becomes consistent for all the times during the outage.

[2]In the global search theory for the refinement phase splitting corresponds to reducing the size of the windows of the activities involved in the contention periods.

4 Conclusions: Performance and Expected PayOff

ROMAN has proven successful since it clearly extends the current functionality offered by existing software tools for outage management:

- All the technological constraints currently used for automatic schedule generation are incorporated. In addition, ROMAN produces schedules satisfying the safety constraints.
- More robust schedules are obtained by guaranteeing feasibility over time windows.
- Very fast schedule generation: the current version of ROMAN handles up to 2,000 activities in approximately 1 minute on a Sparc 2.
- The schedules are often better than the current solutions since many new possibilities are explored.[3]

The current version of ROMAN was completed in November 1995, and it has been demonstrated to several large nuclear power plants such as American Electric Power Service, Baltimore Gas & Electric, PECO Energy, *etc.* The demonstration was successful, and EPRI, a consortium of more than 90% of the utilities in the US, has decided to use the approach embodied in ROMAN to build the next generation of outage scheduling tools — referred to as Advanced Technology Outage Scheduler.

References

[Blazewicz *et al.* 83] J. Blazewicz, J. Lenstra, and A. Rinnooy Kan. Scheduling Projects to Resource Constriants: Classification and Complexity. *Discrete Appl. Math.*, 5:11–24, 1983.

[Gomes 96] Carla O. Pedro Gomes. Integration of Planning and Scheduling. Technical report of Rome Laboratory, Jan. 1996.

[PSDI 94] PSDI. Managing Outages on the Desktop. Technical Brochure, 1994.

[Smith & Parra 93] Doug Smith and Eduardo Parra. Transfornational Approach To Transportation Scheduling. In *Proceedings of the Eigth Knowledge-Based Software Engineering Conference*, Chicago, Illinois, 1993.

[3]Human schedulers tend to aggregate tasks and schedule them as a blocks rather then exploring interesting possibilities that occur when the activities are scheduled separately.

[Smith 87] Douglas R. Smith. Structure and Design of Global Search Algorithms. Technical Report KES.U.87.11, Kestrel Institute, 1987.

[Smith 91] Douglas R. Smith. KIDS: A Knowledge-based Software Development System . In M. Lowry and R. McCartney, editors, *Automating Software Design*, pages 483–514. MIT Press, 1991.

[Smith *et al.* 95] Doug Smith, Eduardo Parra, and Stephen Westfold. Synthesis of High Performance Transportation Schedulers. Technical Report Tech. Rep. KES.U.95.1, Kestrel Institute, 1995.

[Vaessens *et al.* 94] R. J. M. Vaessens, E. H. L. Aarts, and J. K. Lenstra. Job Shop Scheduling by Local Search. Memorandum COSR 94-05, Eindhoven University of Technology, Department of Mathematics and Computing Science, 1994.

[Wallace 90] Ronal C. Wallace. A History of the Project Management Applications in the Utility Industry. *Project Management Journal*, September 1990.

*U.S. GOVERNMENT PRINTING OFFICE: 1997-509-127-61014

MISSION OF ROME LABORATORY

Mission. The mission of Rome Laboratory is to advance the science and technologies of command, control, communications and intelligence and to transition them into systems to meet customer needs. To achieve this, Rome Lab:

a. Conducts vigorous research, development and test programs in all applicable technologies;

b. Transitions technology to current and future systems to improve operational capability, readiness, and supportability;

c. Provides a full range of technical support to Air Force Material Command product centers and other Air Force organizations;

d. Promotes transfer of technology to the private sector;

e. Maintains leading edge technological expertise in the areas of surveillance, communications, command and control, intelligence, reliability science, electro-magnetic technology, photonics, signal processing, and computational science.

The thrust areas of technical competence include: Surveillance, Communications, Command and Control, Intelligence, Signal Processing, Computer Science and Technology, Electromagnetic Technology, Photonics and Reliability Sciences.